

DOUGLAS F. YOUNG, Clerk  
By  
Deputy Clerk

  
 \_\_\_\_\_  
*Judge's signature*  
**Erin L. Wiedemann, Chief United States Magistrate Judge**  
 \_\_\_\_\_  
*Printed name and title*



**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with the Google Drive and Google Photos user ID(s) or email address [jakelankford88@gmail.com](mailto:jakelankford88@gmail.com), as well as any and all account information with telephone number (479) 233-1410; certain accounts that are stored at the premises controlled by Google, Inc. (Google, Inc.) **between the time period of January 01, 2019 until the present** that is stored at premises owned, maintained, controlled, or operated by Google Inc., 1600 Amphitheatre Parkway, Mountain View, California 94043.



**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Google**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google Inc. ("Google"), including any messages, records, files, logs, or information that have been deleted but are still available to Google. Google is required to disclose the following information to the government for each user ID listed in Attachment A:

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Google passwords, Google security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the account and all other documents showing the user's posts and other activities;
- (c) All photos and videos uploaded, distributed, received, or saved by that user ID;
- (d) All profile information, status updates, and contact lists associated with the accounts;
- (e) All other records of communications and messages made or received by the user;
- (f) All "check ins" and other location information;
- (g) All IP logs, including all records of the IP addresses that logged into the account;
- (h) All past and present lists of friends or contacts created by the account;
- (i) Any and All information deleted from the accounts but still recoverable by Google;



- (j) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (k) All privacy settings and other account settings, including privacy settings;

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2251 and Section 2252 involving the suspects outlined herein since **January 01, 2019 until present**, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) Included, but not limited to, any and all sexually explicit images of minors
- (b) Evidence indicating how and when the Google Photos account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Google account owner;
- (c) Evidence indicating the Google Photos account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with the user ID about matters relating to the sexual exploitation of children or involving nude images of children being sent and received via the Internet or other means.



- (f) Any and all conversations, contacts, messages, emails, posts and/or chats involving the solicitation or enticement of minors to engage in sexually explicit conduct and/or encouraging minors to produce images or videos of themselves nude or engaging in sexually explicit conduct. Any and all conversations with others, adult or minors, concerning the sexual exploitation of children or the sending or receiving of images of minors, nude, clothed, or otherwise.



**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
RECORDS PURSUANT TO FEDERAL RULES OF  
EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, LLC and my title is \_\_\_\_\_ . I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google, LLC. The attached records consist of \_\_\_\_\_ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, LLC and they were made by Google, LLC as a regular practice; and

b. such records were generated by Google, LLC electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google, LLC in a manner to ensure that they are true duplicates of the original records; and



2. the process or system is regularly verified by Google, LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

---

Date

---

Signature



**UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF ARKANSAS**

**IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
GOOGLE, LLC ACCOUNT  
[jakelankford88@gmail.com](mailto:jakelankford88@gmail.com) STORED AT  
PREMISES CONTROLLED BY  
GOOGLE, LLC**

No. \_\_\_\_\_

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR SEARCH WARRANT**

I, Thomas Wooten, a Task Force Officer with Homeland Security Investigations (HSI)  
being duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this Affidavit in support of an application for a search warrant for information related to Google email account: [jakelankford88@gmail.com](mailto:jakelankford88@gmail.com), as well as any and all account information for telephone number (479) 233-1410; certain accounts that are stored at the premises controlled by Google, Inc. (Google, Inc.), an e-mail, file storage and synchronization service provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 74043. The information to be searched is described in the following paragraphs and in Attachment A. This Affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, Inc., to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Task Force Officer with the Department of Homeland Security, Homeland



Security Investigations ("HSI"), currently assigned to the Assistant Special Agent in Charge Office in Fayetteville, Arkansas. Since June of 2000, I have been a police officer / detective with the Springdale, Arkansas Police Department. As such, I am authorized by the State of Arkansas to apply for and execute search warrants, arrest warrants and other instruments of the court. As a police officer / detective, I have received specialized training in matters related to criminal investigation, specifically but not limited to the area of sexual exploitation of minors, drug distribution, and money laundering. Since August of 2017, I have been assigned as a Task Force Officer to Homeland Security Investigations (HSI), a component of the U.S. Department of Homeland Security. As a Task Force Officer (TFO) with HSI I primarily investigate crimes related to the sexual exploitation of minors. Prior to joining HSI, I attended a 40-hour training session covering Title 8, Title 18, Title 19 and Title 21 of the United States Code. As such, I am a law enforcement officer within the meaning of Section 115(c)(1) of Title 18 United States Code, who is authorized by law or Government agency to engage in or supervise the prevention, detection, investigation and/or prosecution of any violation of Federal and State criminal law. Since joining HSI as a taskforce officer, your Affiant has received training in Cellebrite Mobile Forensics, Passmark Software/OSForensics Triage tools, and has obtained certifications as a Cellebrite Certified Operator, Cellebrite Certified Physical Analyst and OSForensics Triage Operator.

3. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this Affidavit have been obtained from my first-hand knowledge of events, as well as from other law enforcement officials.

4. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that evidence constituting violations of Title 18, United States



Code, Sections 2252/2252A "Possession of Child Pornography" are currently present on the item described as Attachment A.

5. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband/ fruits of these crimes further described in Attachment B.

#### **DEFINITIONS AND AUTHORITY**

6. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors, which has been defined in Title 18 U.S.C. 2256, as an individual under 18 years of age.

7. Under 18 U.S.C. Section 2252(a)(1) (transportation), 2252(a)(2) (receipt and distribution), and 2252(a)(4)(B) and 2252A(a)(5)(B) (possession), it is a federal crime for any person to transport, distribute, receive, and possess child pornography, as that term is defined by federal law. Further under 18 U.S.C. Section 2253(a)(3), a person who is convicted of an offense under 18 U.S.C. Section 2252 or 2252A, shall forfeit to the United States such person's interest in any property, real or personal, used or intended to be used to commit or to promote the commission of such offense.

#### **BACKGROUND CONCERNING GOOGLE DRIVE AND GOOGLE PHOTOS**

8. Based on my knowledge and experience and information obtained from other law enforcement personnel with training and experience in this area, the following is known about Google Drive and Google Photos accounts:



- a) Google Drive is a file storage and synchronization service created by Google. It allows users to store files in the cloud, share files and edit documents, spreadsheets and presentations with collaborators.
- b) For Google Drive to synchronize files between the user's computer and Google Drive storage, the Google Drive 'client' software must be running on the user's computer. The client communicates with Google Drive to synchronize data.
- c) Google Drive can be accessed offline on the Google Chrome browser via a Chrome application, which can be installed from the Chrome Web Store. Documents, spreadsheets, presentations and drawings can also be viewed and edited offline through standalone Chrome applications.
- d) Google gives every user 15 GB of online storage space, which is shared across three of its most-used services, Google Drive, Gmail and Google+ Photos.
- e) Google Drive incorporates a system of file sharing in which the creator of a file or folder is, by default, its owner. The owner can regulate the public visibility of the file or folder. Files or folders can be shared privately with particular users having a Google account, using their @gmail.com email addresses. Sharing files with users not having a Google account requires making them accessible to anybody with the link. This generates a secret URL for the file, which may be shared via email, blogs, etc. Files and folders can also be made public on the internet, which means that they can be indexed by search engines and thus can be found and accessed by anyone.
- f) Google Photos is a photo sharing and storage service that gives user free, unlimited storage for photos up to 16 MP. Users can search for anything in photos, with the service returning results from three major categories: People, Places and Things.



**PROBABLE CAUSE**

9. On or about October 29, 2019, an ICAC Taskforce Affiliate from the Siloam Springs Police Department received Cyber Tip Line Report Number 55686739 from the National Center for Missing and Exploited Children (Hereinafter referred to as NCMEC), in regards to a Google account that uploaded 44 images of what is believed to be child pornography to the Google account of [jakelankford88@gmail.com](mailto:jakelankford88@gmail.com) through Google Photos and Google Drive. The information on the suspected media containing child pornography was submitted to the Cyber Tip Line by Google Inc. on September 19, 2019 and the lead was subsequently sent to the Arkansas Internet Crimes Against Children Task Force.

10. The cyber tip did not provide the upload IP addresses for the associated child pornography photos, but Google advised they may be able to provide the information with a valid search warrant. The Google email account was also found to be associated with a telephone number of (479) 233-1410. Using open source information, the telephone number in question showed to be used by Jake Lankford several times to call the Siloam Springs Police Department, with the last time being August 6, 2019.

11. The Taskforce Affiliate viewed the reported child abuse images in question and observed 44 digital photographs depicting prepubescent white females. Approximately 40 of the digital photographs were of girls ranging between approximately three (3) years old to approximately 10 years old. The images depicted the girls exposing their vagina and breasts in a sexual manner position. The Taskforce Affiliate viewed all of the files depicting the minors and described three of these files as follows:

(a) Filename hash: 2a5c8887a395344f5d8cea10fce6babe

This image is of an approximate four (4) year old female. The image itself depicts the female lying on her back with her legs spread open with an item inserted partly into her vagina.

(b) Filename hash: 1f09d12aa77d03fca8bc7595e008d1a0



This image is of a sleeping approximate seven (7) year old female. The image itself depicts the nude female leaned back with her legs spread open exposing her vagina and breasts.

(c) Filename hash: f0beeece7b0d629f08fbb138ecfea87e

This image is of a sleeping approximate six (6) year old female. The image itself depicts the female leaned back with her legs spread open exposing her vagina. The female is wearing a shirt which is covering her breasts.

12. During the investigation, it was determined that Jake Lankford used phone number 1-479-233-1410 as his contact phone number with the apartment manager's office where he lives at 1255 W. Tulsa Street 18C, Siloam Springs, Arkansas. Jake Lankford has also called the Siloam Springs Police Department using the phone number 1-479-233-1410. Using the database Accurint, the Taskforce Affiliate was able to verify Jake Lankford uses the email [jakelankford88@gmail.com](mailto:jakelankford88@gmail.com).

13. As a result of this investigation, your Affiant suspects there could be more evidence stored within the Google Photos and Google Drive account belonging to [jakelankford88@gmail.com](mailto:jakelankford88@gmail.com) and personal identifying information regarding the suspect's identity that would assist in the child pornography investigation.

#### **BACKGROUND REGARDING COMPUTERS AND THE INTERNET**

14. Your Affiant has become familiar with the Internet, which is a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state.

15. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail ("e-mail") or Instant Messaging



services (IM). An individual who wants to use the Internet must first obtain an account with a computer or cellular telephone that is linked to the Internet – for example, through a commercial service – which is called an “Internet Service Provider” or “ISP”. Once the individual has accessed the Internet, whether from a residence, a university, a place of business or via their cellular service provider, that individual can use Internet services, including sending and receiving e-mail and IM.

16. The Internet is a worldwide computer network that connects computers and facilitates the communication and the transfer of data and information across state and international boundaries. A user accesses the Internet from a computer network or Internet Service Provider (“ISP”) that connects to the Internet. The ISP assigns each user an Internet Protocol (“IP”) Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 12.345.678.901. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP’s record retention policies.

17. Computers as well create a “Log File” that automatically records electronic events that occur on the computer. Computer programs can record a wide range of events including remote access, file transfers, long/logoff times, systems errors, Uniform Resource Locator addresses (websites), unique searches performed on the Internet and various forms of electronic communications.

18. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto the hard drive, deleted, or viewed via the Internet.



Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten.

19. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.


20. The use of the Internet and more specifically electronic communications via the Internet provides individuals the ability to mask their true identities as well as their physical locations. Additionally, the use of the Internet provides individuals and their associates the ability to access social networking sites free of charge to further their criminal activity.

### **CONCLUSION**


21. Therefore, your Affiant respectfully requests this Court to issue a search warrant authorizing the search of Google Photo and Google Drive account, [jakelankford88@gmail.com](mailto:jakelankford88@gmail.com), as well as any and all account information pertaining to telephone number (479) 233-1410 which is controlled and maintained by Google, Inc., as described in Attachment A, to seize the evidence, fruits, and instrumentalities described in Attachment B, which individually or collectively



constitute violation(s) of Title 18 United States Code, Sections 2252 and 2252A(a)(5)(B) (Possession of Child Pornography).

  
Thomas Wooten, Task Force Officer  
Homeland Security Investigations

Affidavit subscribed and sworn to before me this 6th day of November 2019.

  
Erin L. Wiedemann  
Chief United States Magistrate Judge